

Máster en Informática

Facultade de Informática



Universidade da Coruña

KeyLogging

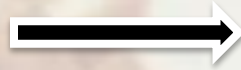
Bruno López Lagares

Seguridad en Sistemas de Información

22-05-2008

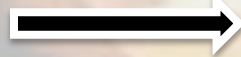
Etimología

Key



Tecla

Log



Grabar / Registrar

¿Qué son?

Software o Hardware que registra las pulsaciones de teclado en un fichero de log

KeyLoggers

Introducción

Evolución

Hardware keyloggers

Software keyloggers

Prevención y protección

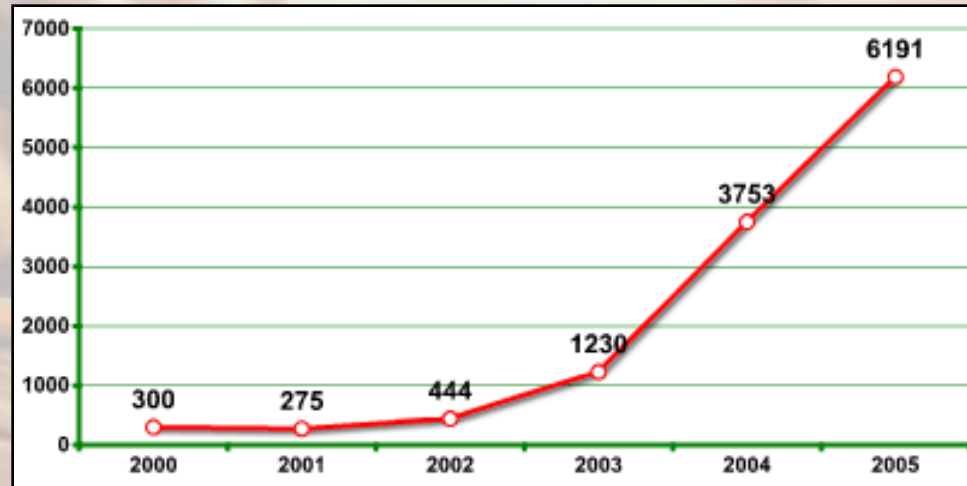
Ejemplo Hardware

Ejemplo Software

Detección

Casos reales

Crecimiento de su uso



Rápido crecimiento del uso de programas maliciosos con funcionalidad de keylogging

[KeyLogging @ Seguridad en Sistemas de Información]

Bruno López Lagares [22-05-2008]



Estadísticas

El 50% de los programas maliciosos detectados el año pasado contenían funciones de keylogging

En EEUU actualmente alrededor de 10 millones de ordenadores están infectados por keyloggers, lo que representan 24.3 millones de dólares en pérdidas

Karspersky generó una de las primeras advertencias sobre estos programas en Junio de 2001 y actualmente cuenta en sus bases de datos con registros de más de 300 familias de keyloggers.

Introducción

Son dispositivos físicos que realizan la función de grabación de la pulsaciones que se realizan en el teclado

Tienen la ventaja de que comienzan el registro en el momento en el que se enciende el ordenador

Normalmente necesitan dos accesos a la máquina objetivo, el primero para su instalación y el segundo para la recuperación del dispositivo

Existen varios tipos, aunque los más comunes son los denominados Adaptadores.

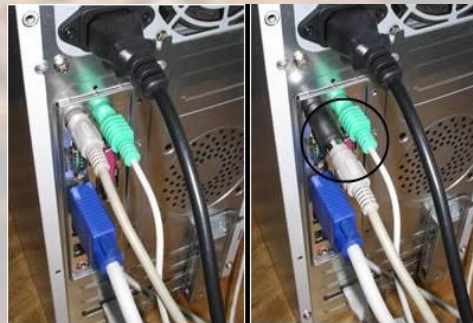
Tipos (I)

Existen 6 tipos:

Adaptadores, Dispositivos, Teclados keylogger, Wireless keyloggers, Wireless keylogger sniffers, Acústicos

Adaptadores

**Se enchufan en el conector del teclado
Pueden ser detectados fácilmente
Toman la apariencia de un balun
para evitar su detección**



Tipos (II)

Dispositivos

Se instalan dentro de los teclados estándar

Requieren habilidad para soldar y acceso al teclado a modificar

Son indetectables a menos que se abra el cuerpo del teclado.

Teclados keylogger

Teclados previamente preparados, con el keylogger ya integrado

Wireless keyloggers

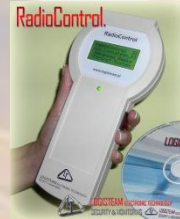
Son monitorizados y controlados mediante una comunicación wireless



Tipos (y III)

Wireless keylogger sniffers

Estos keyloggers reciben paquetes de datos transferidos entre un teclado inalámbrico y el receptor, y después intentan descifrar la clave de seguridad de la comunicación entre ambos



Acústicos

Usan métodos estadísticos similares a los empleados en el desciframiento, haciendo posible identificar que patrón de pulsación está relacionado con que carácter del teclado. Necesitan una grabación bastante larga (1000 o más pulsaciones) para que la estadística sea significativa

Introducción

Son programas diseñados para, en secreto, controlar y registrar cada pulsación del teclado

Los programas legítimos pueden tener una función de keylogger que se puede utilizar para iniciar ciertos programas mediante combinaciones de teclas ('hotkeys')

Hoy en día los keyloggers se usan principalmente para robar información relacionada a varios sistemas de pago online.

Asimismo, muchos keyloggers se esconden en el sistema, por ejemplo, camuflándose como rootkits, lo cual los convierte en programas troyanos completamente furtivos.

Tipos (I)

Existen 2 grandes tipos:

Acceso local (Basados en núcleo, Hooked y Métodos creativos) y Acceso Remoto

Acceso Local

Basados en Núcleo:

Acceden al núcleo del sistema operativo y tienen casi siempre acceso autorizado al hardware , lo que los hace de gran alcance (e.g. haciendo el papel de driver)

Son difíciles de escribir y de combatir

Hooked:

Se vinculan al teclado con las funciones proporcionadas por el sistema operativo

Tipos (y II)

Métodos creativos:

En este tipo el programador utiliza funciones como GetAsyncKeyState, GetForegroundWindow

Son los más fáciles de escribir, pero como requieren comprobar el estado de cada tecla varias veces por segundo, pueden causar un aumento sensible en el uso de la CPU y pueden ocasionalmente dejar sin registrar algunas pulsaciones.

Acceso Remoto

Se utiliza el software local programado con una característica añadida para transmitir los datos registrados en el ordenador objetivo y sitúa los datos disponibles en una ubicación remota (FTP, web, correo electrónico, ...)

Hardware

Métodos a realizar:

Para detectar estos dispositivos nos basta con realizar un análisis visual de la conexión entre el teclado y el ordenador

Prohibir el acceso físico a los ordenadores más sensibles, por ejemplo cerrando el cuarto de servidores

Si el ordenador no está a la vista, el principal método de prevención es el siguiente:

Escribimos partes de la contraseña, después en un editor de texto seguimos escribiendo lo que serán caracteres basura, y á continuación escribiremos el resto de la contraseña. De este modo evitaremos que se registre la contraseña de modo nítido

KeyLoggers

Introducción

Evolución

Hardware keyloggers

Software keyloggers

Prevención y protección

Ejemplo Hardware

Ejemplo Software

Detección

Casos reales

Software (I)

Métodos a realizar:

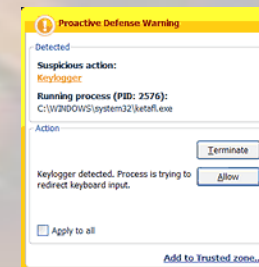
Contraseñas de uso único

Por medio de un Token o de una calculadora:



Sistema con protección proactiva

Se advierte al usuario de las posibles acciones a ejecutar o cancelar



[KeyLogging @ Seguridad en Sistemas de Información]

Bruno López Lagares [22-05-2008]



Software (y II)

Teclado virtual

Están pensados para personas discapacitadas y no explícitamente para resolver el problema del keylogging

Actualmente hay métodos como el screenlogging que hacen inútil esta opción



Podemos ver un ejemplo de cómo este método está obsoleto en : http://www.hispasec.com/laboratorio/cajamurcia_en.htm

Keylogger Hardware DIY (I)

Pasos para la construcción del keylogger

- **Programar el firmware del microcontrolador**
- **Estañar los componentes, comenzando por el microcontrolador y la memoria EEPROM**
- **Estañar los conectores PS/2 al keylogger**
- **Cubrir el keylogger con el tubo termorretráctil**



Keylogger Hardware DIY (II)

Pasos Modo registro

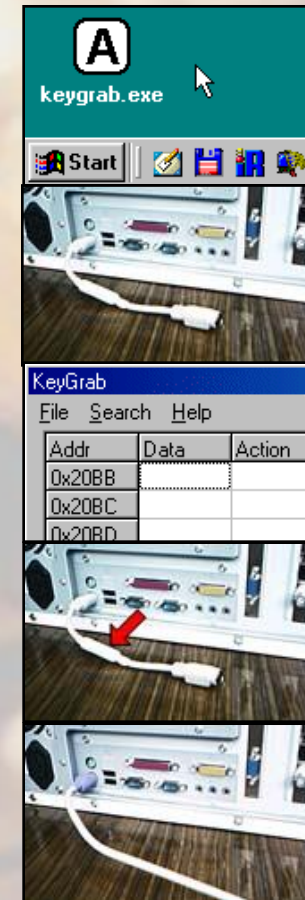
- **Localizar el conector PS/2 entre el teclado y el ordenador**
- **Desenchufar el teclado**
- **Conectar el keylogger por hardware en el adaptador del teclado**
- **Conectar el teclado al keylogger**



Keylogger Hardware DIY (III)

Pasos Modo playback

- **Ejecutar la aplicación KeyGrab**
- **Conectar el keylogger
(Con el teclado desenchufado)**
- **Hacer click en la barra de título
de la aplicación para activarla**
- **Presionar el pulsador del keylogger
para la descarga de datos a la
aplicación**
- **Desconectar el keylogger hardware
y volver a conectar el teclado**



Keylogger Hardware DIY (y IV)

Análisis de datos

- 1] Posición del dato en la memoria hardware del keylogger***
- 2] Pulsación de tecla registrada y guardada.**
- 3] Incidencia - pulsación o liberación de tecla.**
- 4] Scan code de pulsación de tecla en el bus PS/2***
- 5] Última posición grabada durante el registro en la memoria***
- 6] Tamaño de la memoria hardware del keylogger (en kilobits).**

Addr	Data	Action	Key
0x20BB			
0x20BD	1a	Pressed	Z
0x20BD	31	Released	N
0x20BE	f0		
0x20Bf	31	Pressed	N
0x20C0	35	Released	Y
0x20C1	f0		
0x20C2	35	Pressed	Y
0x20C3	29	Released	SPACE
0x20C4	f0		
0x20C5	29	Pressed	SPACE
0x20C6	2c	Pressed	T
0x20C7	24	Released	E
0x20C8	f0		
0x20C9	2c	Released	T
0x20CA	f0		
0x20CB	24	Pressed	E
0x20CC	1b	Released	S
0x20CD	f0		
0x20CE	1b	Pressed	S
0x20CF	2c	Released	T
0x20D0	f0		

Memory : 256kbit Last address : 0x20d7

(* Formato Hex)

KeyLoggers

Introducción

Evolución

Hardware keyloggers

Software keyloggers

Prevención y protección

Ejemplo Hardware

Ejemplo Software

Detección

Casos reales

Código en C

Se utilizan las funciones:

GetActiveWindow

GetWindowText

GetKeyNameText

GetKeyboardState

Al detectar las pulsaciones de teclado se escribe en un fichero de log la tecla pulsada

[KeyLogging @ Seguridad en Sistemas de Información]

Bruno López Lagares [22-05-2008]



Revealer Keylogger (I)

Existen tanto la versión Free (Gratuita) como la Pro (24.90€)

No requiere instalación

Es posible poner la carpeta en modo

Se inicia automáticamente al encender el ordenador

Es posible cambiarle el nombre al ejecutable para ocultarlo aún más en el administrador de tareas y así confundirlo con procesos del sistema, por lo que la mayoría de los antivirus no lo detectan.

KeyLoggers

Introducción

Evolución

Hardware keyloggers

Software keyloggers

Prevención y protección

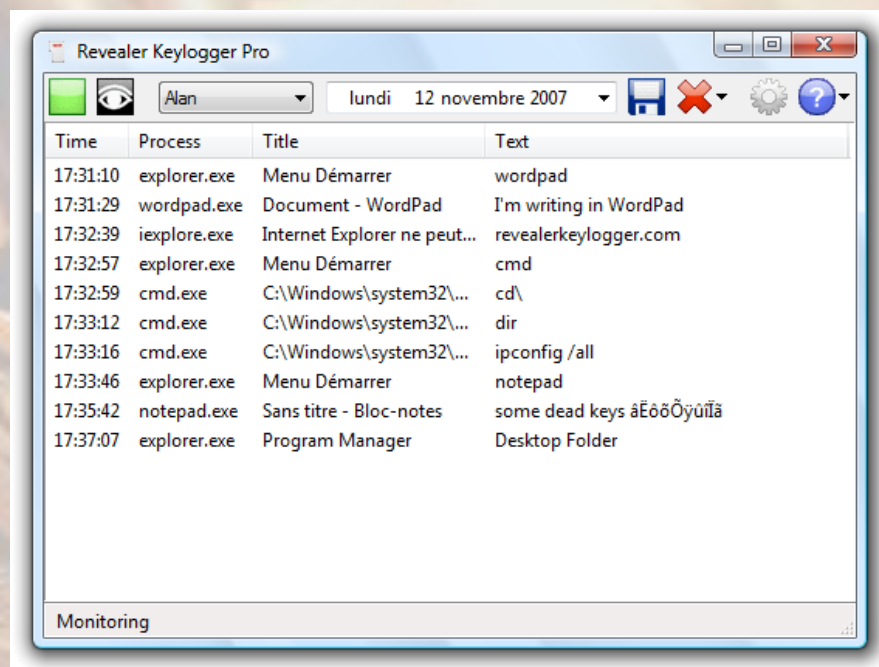
Ejemplo Hardware

Ejemplo Software

Detección

Casos reales

Revealer Keylogger (II)



Apariencia del Revealer Keylogger en su versión Pro

[KeyLogging @ Seguridad en Sistemas de Información]

Bruno López Lagares [22-05-2008]



KeyLoggers

Introducción

Evolución

Hardware keyloggers

Software keyloggers

Prevención y protección

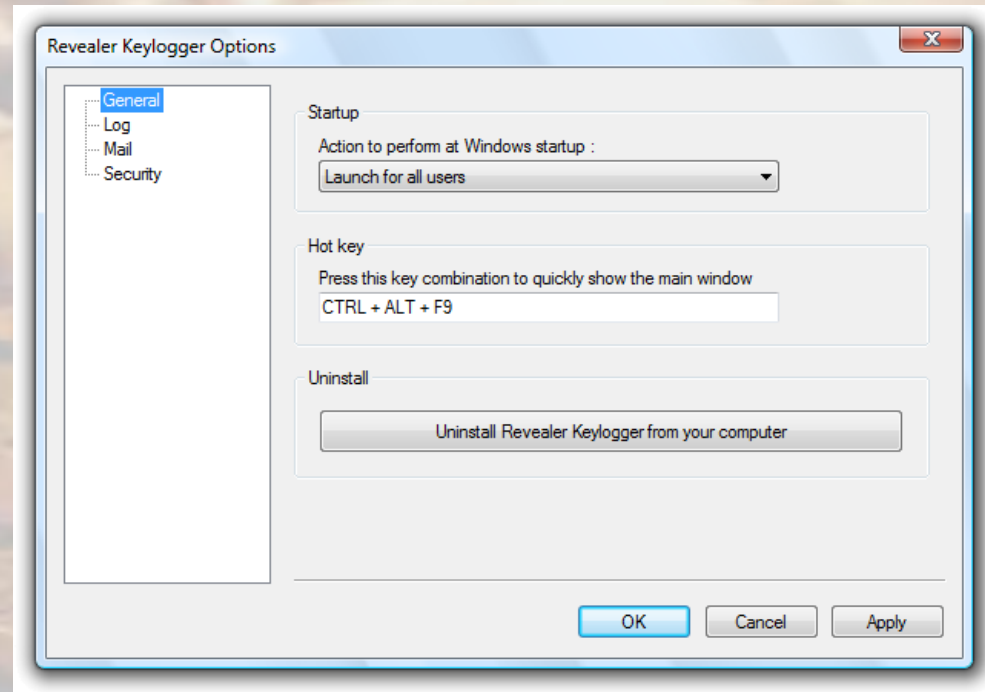
Ejemplo Hardware

Ejemplo Software

Detección

Casos reales

Revealer Keylogger (III)



Opciones → General

Opciones de arranque
Hot Keys
Desinstalación

[KeyLogging @ Seguridad en Sistemas de Información]

Bruno López Lagares [22-05-2008]



KeyLoggers

Introducción

Evolución

Hardware keyloggers

Software keyloggers

Prevención y protección

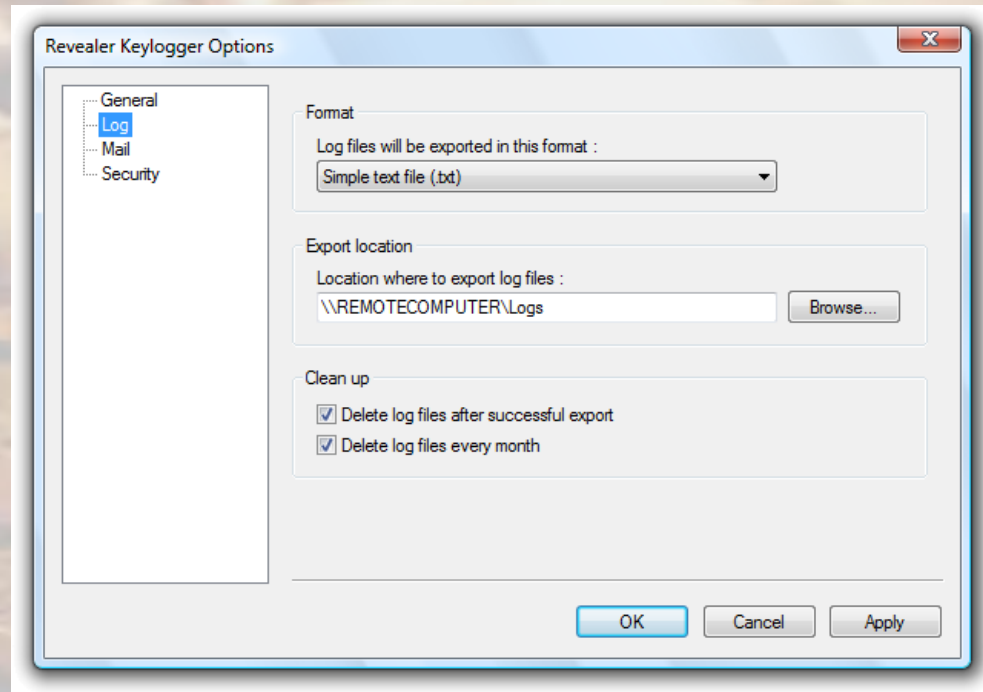
Ejemplo Hardware

Ejemplo Software

Detección

Casos reales

Revealer Keylogger (IV)



Opciones → Log

Formato del log
Exportación del log
Opciones de borrado

[KeyLogging @ Seguridad en Sistemas de Información]

Bruno López Lagares [22-05-2008]



KeyLoggers

Introducción

Evolución

Hardware keyloggers

Software keyloggers

Prevención y protección

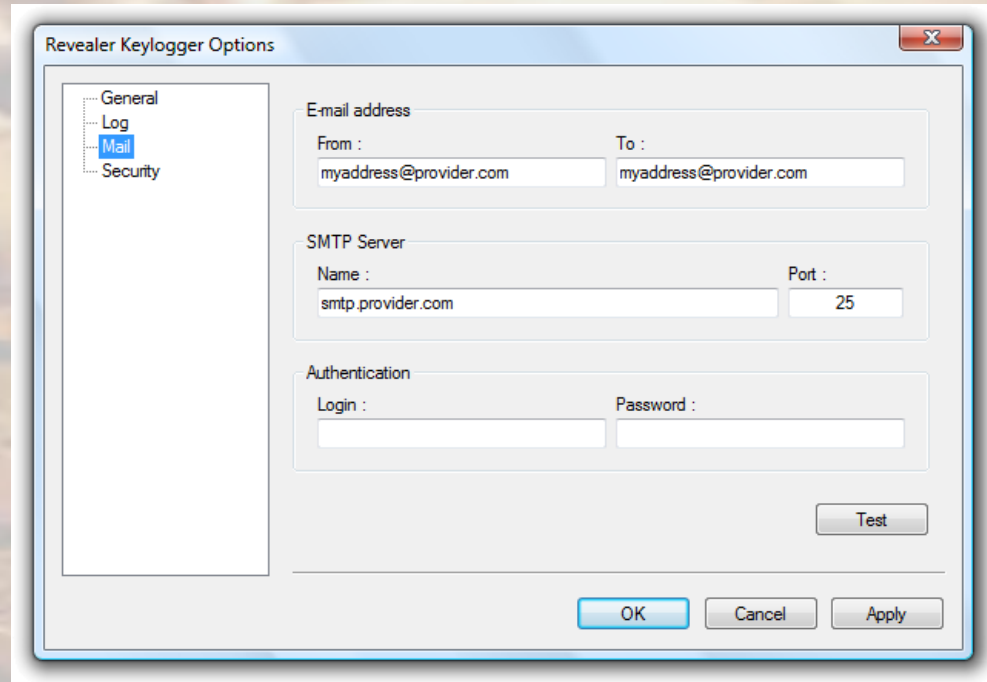
Ejemplo Hardware

Ejemplo Software

Detección

Casos reales

Revealer Keylogger (V)



Opciones → Mail

[KeyLogging @ Seguridad en Sistemas de Información]

Bruno López Lagares [22-05-2008]



KeyLoggers

Introducción

Evolución

Hardware keyloggers

Software keyloggers

Prevención y protección

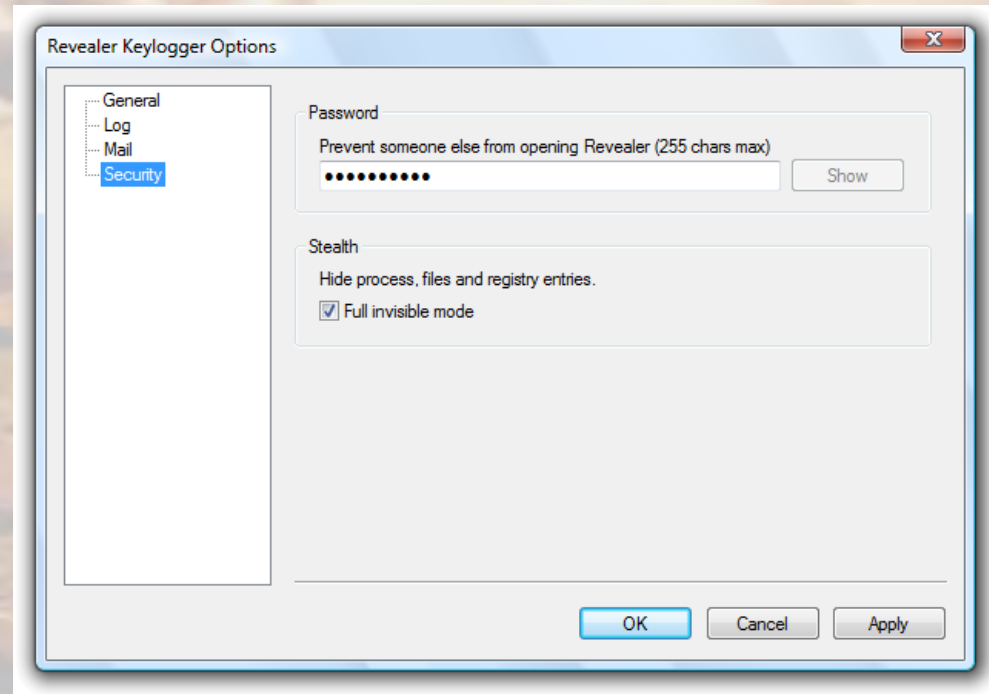
Ejemplo Hardware

Ejemplo Software

Detección

Casos reales

Revealer Keylogger (y VI)



Opciones → Security

Contraseña
Ocultación

[KeyLogging @ Seguridad en Sistemas de Información]

Bruno López Lagares [22-05-2008]



Hardware

El principal método (teniendo acceso físico) es la inspección visual

Si la inspección visual no es satisfactoria debemos utilizar software para detectar el keylogger

Software

Existen diferentes métodos para la detección de keyloggers (válidos tanto para hardware como software):

Detección mediante las bases de datos de firmas

Defensa proactiva

Bloqueo de instalación de una rutina de procesamiento de interrupción

Bloqueo de solicitudes cíclicas sobre el estado del teclado

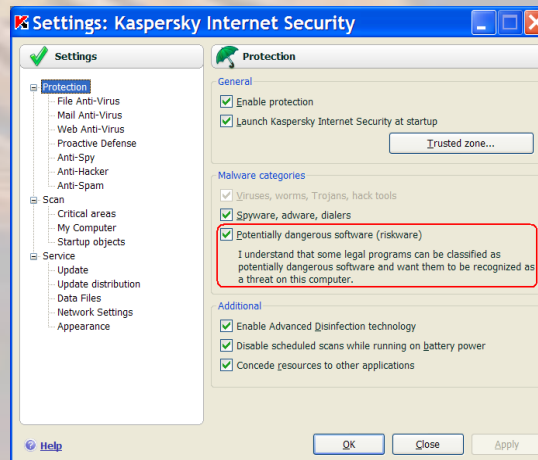
Detección de procesos ocultos en el registro de pulsaciones de teclado

Métodos Software (I)

Bases de datos de firmas

Debido a que ciertas funciones de keylogging pueden ser legítimas, los antivirus engloban estas funciones en el apartado de “Software potencialmente peligroso”

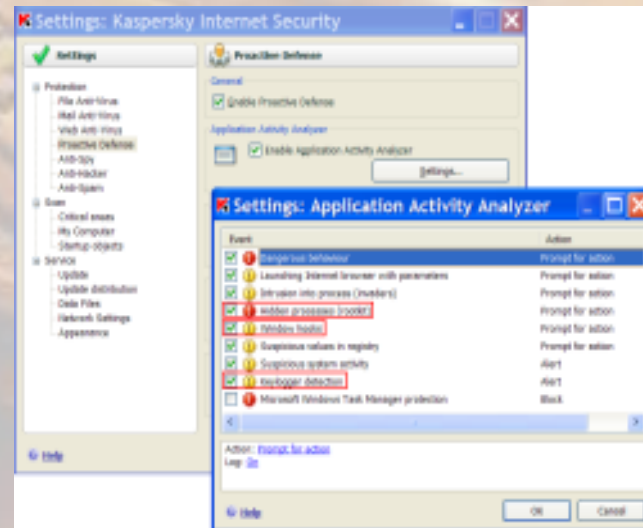
Se utilizan las bases de datos de los antivirus para detectar y neutralizar las funciones keylogging



Métodos Software (II)

Defensa proactiva

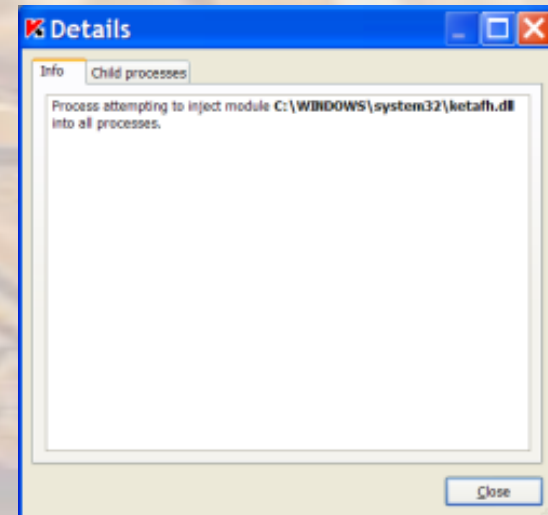
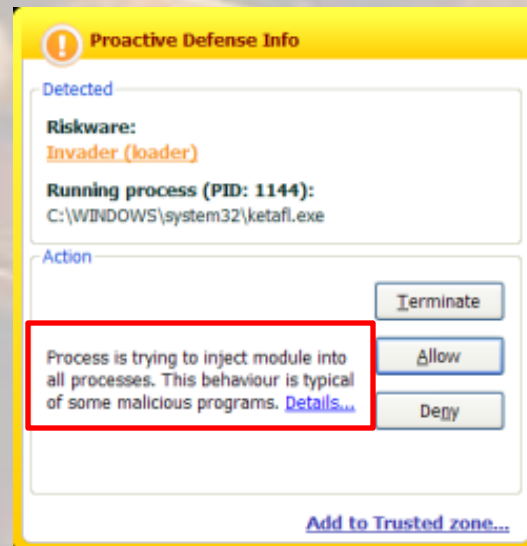
La defensa proactiva protege al usuario contra las nuevas amenazas y contra las nuevas variantes de los programas maliciosos sin necesidad de actualizar las bases de datos, porque funciona bajo el principio de la monitorización continua de actividades



Métodos Software (III)

Bloqueo de instalación de una rutina de interrupción

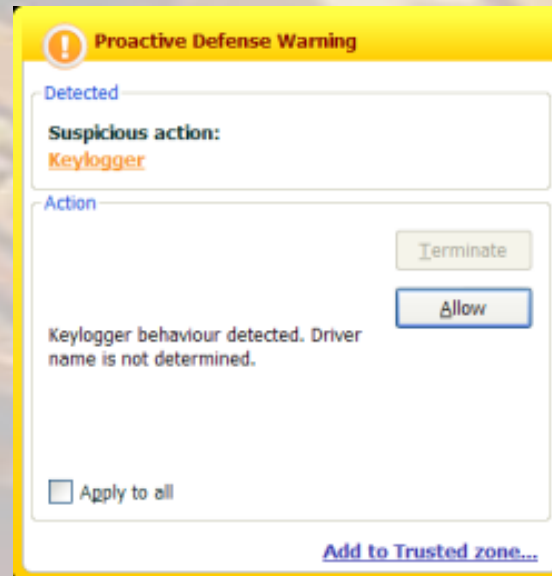
Consiste en interceptar la instalación de una rutina de captura de las actividades del el teclado que es realizada mediante la función SetWindowsHook



Métodos Software (IV)

Bloqueo de solicitudes cíclicas sobre el estado del teclado

Consiste en interceptar las solicitudes cíclicas sobre el estado del teclado mediante la función `GetAsyncKeyState`



Métodos Software (y V)

Detección de programas ocultos en el registro de pulsaciones de teclado

Se encubre el proceso ejecutable que realiza el keylogging mediante la acción del driver ketaf.sys, el cual bloquea las llamadas de dos funciones de enumeración de la lista de procesos y de la lista de archivos en el núcleo del sistema operativo

Este método consiste en bloquear dicho ejecutable encubierto



Banco Nordea

En Agosto de 2006, numerosos clientes de este gran banco escandinavo, comenzaron a recibir correos electrónicos ofreciendo una oferta para instalar un producto antispam adjunto al mensaje.

El producto realmente instalaba un troyano (Haxdor) en el ordenador con una función de keylogging

Al entrar en la web online del banco, al ingresar los datos de usuario, el troyano lanzaba un error y solicitaba reingresar los datos de cliente, los cuales eran grabados y enviados al servidor del ciberdelincuente

La propagación del troyano con función de keylogging originó que fueran robados más de un millón de dólares de las cuentas de los clientes

Rani Rahay

Un matrimonio israelí, elaboró un programa con función de keylogging ‘encargado’ por compañías como Cellcom, Pelephone y el proveedor de TV por satélite YES

El programa fue utilizado para la obtención de datos de la agencia de relaciones públicas Rani Rahay, cuyos clientes eran tan importantes como Partner Communications (el segundo proveedor de telefonía móvil en Israel)

También fue sospechosa la compañía de importación de coches Mayer de cometer espionaje industrial contra Champion Motors

El creador del programa fue condenado a 2 años de cárcel, mientras que su mujer, que fue responsable de la venta, fue condenada a 4 años

Máster en Informática

Facultade de Informática



Universidade da Coruña

KeyLogging

Gracias

¿Alguna pregunta?

Bruno López Lagares

Seguridad en Sistemas de Información

22-05-2008